Etude pour le CREOGN :
Données personnelles et collectivités territoriales : usages actuels et recommandations

I. Cadre de l'étude

1) Les auteurs :

- ***Anne Le Hénanff****, maire-adjointe en charge de la communication, des systèmes d'information et du développement numérique de la ville de Vannes, Réserviste Citoyenne Cyber.*
- ***Didier Danet,*** *responsable du pôle Mutation des Conflits, CREC Saint-Cyr, membre de la Chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales.*
- ***Gérard de Boisboissel****, ingénieur de recherche, CREC Saint-Cyr, secrétaire général de la Chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales.*

2) Les communes sollicitées :

- 2 communautés de communes de 20 000 et 85 000 habitants
- 2 communes de taille moyenne (entre 50 et 100 000 habitants)
- 1 commune de petite taille (moins de 20 000 habitants)
- 4 communes de très petite taille (entre 1 et 5 000 habitants), typique du monde rural.

3) Propos liminaires :

Cette étude est propriété de la **Gendarmerie Nationale**, commanditée par le CREOGN.

Elle a été réalisée de septembre 2017 à décembre 2017. Les mois de septembre et d'octobre ont principalement servi à prendre contact avec les collectivités territoriales et à récupérer les données nécessaires à l'étude.

Il est à noter que les collectivités concernées ont pris sur leur temps de travail pour répondre à notre sollicitation, qu'elles ont fait cette étude avec sérieux, sérieux qui représente parfaitement le bel esprit de service qui les anime.

Contenu

II. Introduction :

Les collectivités territoriales (ci-après CT) ont le sentiment d'être livrées à elles-mêmes sur les questions de cybersécurité. Elles sont en attente d'un accompagnement et d'un soutien. Elles ont donc été accueillantes lors des entretiens proposés par les rédacteurs pour traiter de la question des usages des données personnelles au sein de leur collectivité, et très à l'écoute sur les futures exigences de protection de ces données qu'imposera le règlement européen pour la protection des données personnelles (RGPD) ainsi que les moyens nécessaires à mettre en œuvre, qu'ils soient techniques ou humains.

Il convient avant tout de faire un distinguo entre données personnelles et données communales, ces dernières ne faisant pas partie de notre étude. Il nous est rapidement apparu que les données personnelles sont très présentes dans les traitements effectués par les collectivités, avec des types divers en fonction des métiers qui les utilisent.

Le croisement de toutes ces données, s'il pouvait être effectué, permettrait de profiler précisément une personne ainsi que toute sa famille et son environnement. Fort heureusement, et pour rappel, les agents publics ont devoir de réserve et de secret sur les données qu'ils utilisent. La CNIL, quant à elle, régule les usages et la diffusion des données personnelles au sein même de la structure.

Enfin, si la numérisation est très avancée d'une façon générale sur notre territoire, il est important de souligner que près de 80% des données dans les petites communes sont stockées sous format papier et que nombre de données personnelles saisies sous format informatique ont été reçues sous format papier dans le même temps.

III. Type de données et classification

Seront listés dans ce chapitre, sous la forme d'une synthèse des données collectées dans les collectivités rencontrées, les types de données personnelles utilisées par ces collectivités.

1) Définition des données personnelles

La définition d'une donnée à caractère personnel selon l'article 2 de la loi du 6 janvier 1978 est la suivante :

> ***« Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».***

a) La notion de « données personnelles »

Dans cette étude, la notion de « données personnelles » est entendue dans le sens qui lui a été donné pour l'application de la loi « Informatique et liberté ».

Il ne s'agit pas de se situer dans la perspective de celui qui voudrait mettre en œuvre un traitement considéré par lui comme légitime au regard de ses activités et qui n'aurait pas le sentiment de violer l'intimité des personnes dont les données font l'objet du traitement, notamment lorsque ces données sont mises à la disposition de tout un chacun par les personnes elles-mêmes. Les informations les plus intimes dévoilées sur des sites comme Facebook, Linkedin, Meetic… Ainsi, les services techniques d'une commune qui souhaiteraient informer les habitants d'un quartier d'une opération d'élagage en leur envoyant un courrier électronique seraient amenés à traiter des informations personnelles pour ce faire : nom, prénom, adresse électronique... Le responsable du service aurait certainement le sentiment de réaliser une opération légitime, utile pour les habitants, répondant à la volonté de mieux communiquer avec les administrés… Il n'en traiterait pas moins des informations personnelles soumises à un régime particulier de protection.

b) Le contenu des données

La notion de « donnée personnelle » doit donc être entendue dans un sens large. Elle englobe la notion « d'informations nominatives » qui était retenue à l'origine par la loi « Informatique et liberté », notion dont la CNIL donnait déjà une interprétation extensive : nom ou numéro de téléphone par exemple, mais aussi appels enregistrés sur le lieu de travail ou carte de transport.

Les « données à caractère personnel » ou « données personnelles » sont aujourd'hui définies de la manière suivante : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». Sont donc visées des informations relatives à l'état de la personne mais aussi à sa situation économique, sa vie sociale… La nouvelle formulation permet notamment d'étendre le domaine des données personnelles à la voix et à l'image, données massivement traitées par les nouvelles technologies de l'information. (par exemple, l'image d'une personne physique enregistrée par une caméra).[1]

c) Les moyens d'identification

Au-delà du contenu des données, il convient pour définir l'étendue de la notion de « données personnelles » de tenir compte des moyens disponibles pour déterminer si une personne est identifiable ou non grâce à ces données. Or, de ce point de vue, les progrès techniques enregistrés depuis le vote de la loi « Informatique et liberté » ont démultiplié les capacités d'identification des individus. Dans un avenir très proche, la généralisation des applications de l'intelligence artificielle leur feront franchir une nouvelle étape. Au regard des moyens ainsi disponibles, la notion de « données personnelles » a vocation à s'étendre de manière significative. Sauf si le système utilisé pour le traitement interdit, par défaut ou par une volonté déterminée, toute identification, « il en résulte que la notion de « données à caractère personnel » ou de « données personnelles » a vocation à englober presque toute information qui se rapporte – de près comme de loin – à la personne dont les données sont traitées. Cela signifie surtout que rares sont les cas où, en définitive,

1 CJUE, 11 décembre 2014, aff. C-212-13, Nejvyšší správní soud (République tchèque) point 22 : A propos d'un système de caméra fixe installé par une personne à des fins de protection de son domicile, la CJUE dispose : « Dès lors, l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel au sens de la disposition visée au point précédent dans la mesure où elle permet d'identifier la personne concernée ».

les opérations effectuées par les exploitants dans le cadre de leurs activités ne portent pas sur des données personnelles »[2] .

d) Synthèse

Il en résulte que sont ou peuvent être des « données à caractère personnel » (liste non exhaustive) :

- Les éléments d'identification d'une personne : nom, prénom, âge, sexe, numéro de passeport, matricule interne d'une entreprise…
- Les identifiants liés aux NTIC : adresse IP[3], coordonnées électroniques, photo ou vidéos d'une personne, appels passés par elle…
- Les données permettant indirectement d'identifier une personne : numéro de sécurité sociale, coordonnées bancaires, diplômes, situation géographique…

On insistera sur le fait que, malgré l'interprétation large donnée par les juges pour favoriser la protection des libertés individuelles, toute donnée énumérée ci-dessus ne présente pas nécessairement et systématiquement un caractère personnel. Encore faut-il qu'elle permette l'identification de la personne directement ou à travers un moyen d'identification disponible. Classiquement, un nom de famille très courant peut ne pas être considéré comme une donnée permettant l'identification d'une personne dans une population. Des données purement factuelles ou quantitatives, comme celles recueillies dans un sondage, ne seront pas considérées comme des données personnelles.

2) Définition d'une donnée sensible

Au sein de cet ensemble très vaste que constituent les « données personnelles » et qui font l'objet d'une protection particulière, certaines présentent un caractère « sensible » car elles touchent à l'intime le plus profond des individus. Elles font l'objet d'un régime de protection renforcée : interdiction de principe du traitement de ces données sauf exception légale.

> « Les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. » ***(Art. 8 loi I&L).***

Ce texte fait l'objet d'une interprétation extensive de la part des juridictions.

---

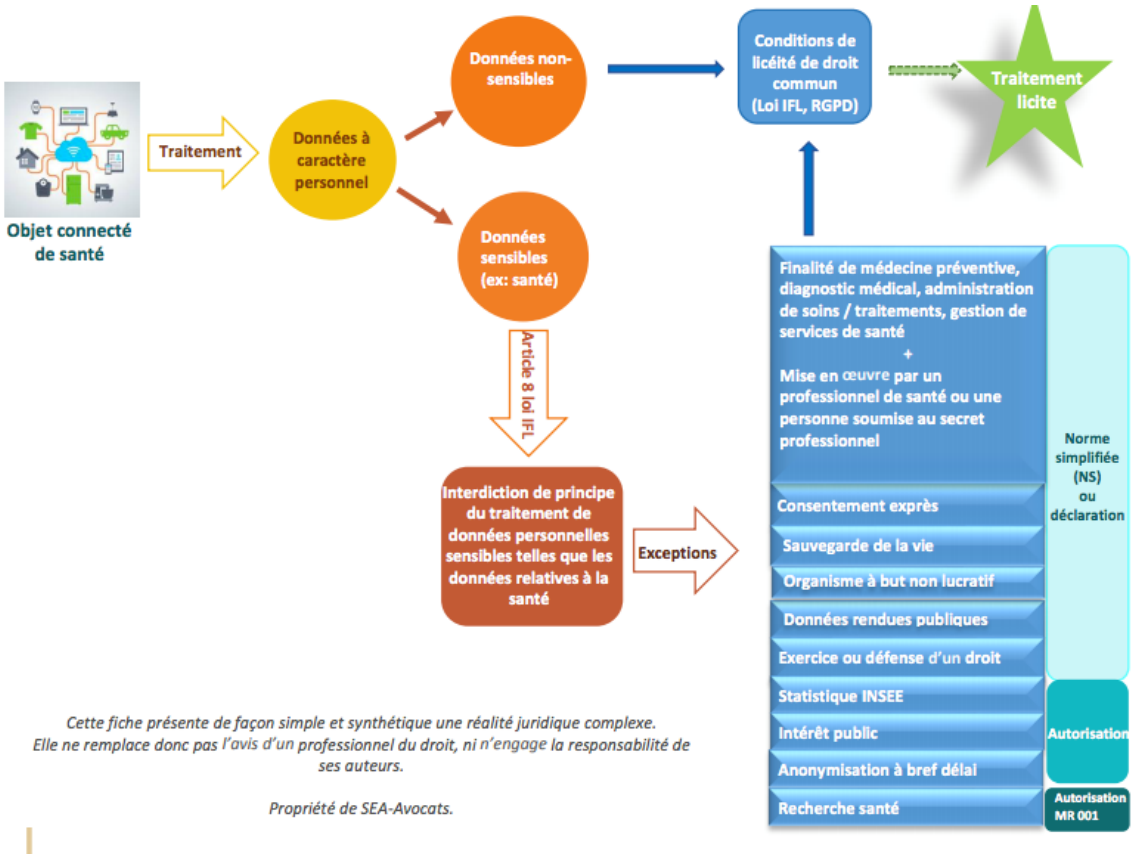
2 Costes Lionel & alii, Lamy Guide du numérique, n°4072

3 Civ.1ère, 3 nov. 2016, Peterson c/ Logisneuf, JCP G no 49, 5 déc. 2016, 1310, note Perray R. : « l'arrêt retient que l'adresse IP, constituée d'une série de chiffres, se rapporte à un ordinateur et non à l'utilisateur, et ne constitue pas, dès lors, une donnée même indirectement nominative ; qu'il en déduit que le fait de conserver les adresses IP des ordinateurs ayant été utilisés pour se connecter, sans autorisation, sur le réseau informatique de l'entreprise, ne constitue pas un traitement de données à caractère personnel ; qu'en statuant ainsi, alors que les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL, la cour d'appel a violé les textes susvisés ; »

« L'indication du fait qu'une personne s'est blessée au pied et est en congé maladie » est ainsi une donnée de santé.[4] Ici encore, si la jurisprudence se veut protectrice des libertés personnelles, elle peut considérer qu'une donnée en relation avec la santé d'une personne n'est pas sensible si elle ne donne pas d'information sur cette personne. Ainsi, la donnée relative au taux d'invalidité du conjoint ne donne pas d'information sur la nature du handicap qu'il subit.[5]

Illustration : exemple des données de santé

Le schéma suivant illustre ce que peut être le traitement des données de santé recueillies à travers un objet connecté.



4 CJCE, 6 nov. 2003, Lindqvist, aff. C. 101/01, D. 2004, p. 1062, obs. Burgogue-Larsen L. L'arrêt intervient à propos d'une dame Lindqvist qui créé, à son domicile et avec son ordinateur personnel, des pages Internet dans le but de permettre aux paroissiens préparant leur confirmation d'obtenir facilement les informations dont ils pouvaient avoir besoin. Des poursuites sont engagées par le Ministère public suédois. La CJCE est saisie. « Par sa quatrième question, la juridiction de renvoi demande si l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46. Eu égard à l'objet de cette directive, il convient de donner à l'expression «données relatives à la santé» employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne. Il convient donc de répondre à la quatrième question que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46. »

5 CE, 28 mars 2014, SNES, Tesson F., AJDA 27 oct. 2014, n° 36, note Salen P. et Perray R.

Source : SEA Avocats, https://www.sea-avocats.fr/medias/org-70/site-102/doc/fiche-sea-donnees-sensibles-18_07_2016.pdf

3) La collecte des données personnelles

Les communes sont relativement libres sur les pratiques de collecte de données. Il existe une très grande variété de pratiques.

Pour la collecte des données et leur récupération, beaucoup de mairies conservent la possibilité pour les citoyens (et même surtout les agents) d'utiliser le papier si ces derniers ne sont pas à l'aise avec le numérique. On estime à 18% aujourd'hui le nombre de personnes qui ne sont pas en mesure d'utiliser des équipements numériques et/ou de les utiliser.

Certaines C.T ont développé le tout numérique et offrent des portails d'accès avec des télé-formulaires pour saisir les données. La dématérialisation y est effectuée de bout en bout. Les transactions financières par internet sont chiffrées.

A noter que les données les plus couramment saisies, et très souvent avec une grande redondance, sont les copies de pièces d'identité, de justificatifs de domicile, de factures, de certains courriers.

Enfin les règles sont très souples sur le stockage et la gestion des données par les C.T et certaines données sensibles ne sont conservées que sous format papier.

Un entretien dans une commune montre assez précisément la façon dont les données personnelles sont collectées par cette ville. La collecte est le plus souvent effectuée sur les lieux d'accueils au public de la ville. Elle peut néanmoins s'effectuer par téléphone, ou par d'autres formes d'échanges : courriers/mails/internet.

Le traitement est très variable selon les cas, la plupart du temps elle est faite en direct, en guichet d'accueil au public, avec saisie par un agent de la ville. Ce peut aussi être après-coup sur saisie des formulaires papiers/mails. Les télé procédures se développent de plus en plus.

Les données saisies par le citoyen sur un portail citoyen sont soient ressaisies par les services soient injectées directement dans un logiciel métier de secteur.

Les mairies offrent toujours l'alternative des moyens de démarches. Ainsi, si un usager ne veut pas passer par une télé procédure, la collecte peut être faite oralement.

4) Classification des données personnelles

Ayant explicité les définitions de ce que sont les données personnelles et les données sensibles, ce paragraphe propose d'apporter une classification des données personnelles en fonction des différentes informations traitées et stockées par les C.T :

Classification de l'ensemble des données personnelles :

données individuelles	nom, prénom, date de naissance, lieu de naissance, nationalité, adresse postale, téléphone(s), @mail ;
données état civil	données individuelles + naissance, mariage (témoins, professions, …), PACS, filiation, décès ;
données familiales	aides sociales, CAF, relations familiales et liens de famille, données de patrimoine ;
données biométriques	empreintes digitales, photo ;
données médicales	numéro de sécurité sociale, fiche médicale fournie par la famille, certificat médical, régime alimentaire, handicap ;
données RH	CV, position, ancienneté, statut, absences, maladies, arrêts maladies, accidents de travail, sanctions, type de véhicule pour remboursement, situation de santé des conjoints ou enfants en vue d'ouverture de droits;
données financières	RIB, dettes, non-valeur ;
données imposition	revenus fiscaux, quotient familial, données de redevance des ordures ménagères;
données urbanisme	propriété des parcelles, location ;
données concession	lieu de la concession funéraire au cimetière, places disponibles ;
données police municipale	suivi de délinquance, infractions, verbalisation, pièces d'identité, n° immatriculation véhicule, contrat d'assurance.

Il est à noter que les données individuelles sont omniprésentes dans toute opération concernant une personne physique. Et de fait, ce sont les données de base qui sont le plus souvent accessibles par tout un chacun via Internet ou via les réseaux sociaux (au travers des pages blanches notamment).

Les données personnelles sensibles au regard de la loi :

Parmi les données de la classification ci-dessus, certaines sont considérées comme étant sensibles au regard de la loi:

- Les données médicales pour EHPAD : dossier médical contenant :
  - maladies, pathologies, anatomo-pathologie (anapath), infections, déclarations obligatoires auprès des pouvoirs publics pour ce qui touche à la contagion, projet d'accompagnement individuel « PAI » dont allergies graves, état de démence, santé psychiatrique, contention médicale, analyse de sang, consentement éclairé de fin de vie, régime alimentaire, libellé de diagnostics visibles au travers du traitement ;
- Dossier enfant avec une partie médicale qui contient une partie des données médicales pour sa prise en charge dans le milieu éducatif ou sa prise en charge par la mairie avant et après les horaires péri ou extra scolaires (multi accueils, vacances, accueil de loisirs sans hébergement « alsh »): les directrices de crèche ont accès à ces données, ainsi que les responsables multi accueils. Ce dossier enfant peut contenir :

    - maladies, pathologies, déclarations obligatoires auprès des pouvoirs publics pour ce qui touche à la contagion, infections, vaccinations, projet d'accompagnement individuel « PAI » dont allergies graves, troubles du comportement et de l'envahissement « TED : autisme, hyperactivité etc. », régime alimentaire), traitements en cours.
- Certaines données RH : Parmi les données contenues dans les dossiers professionnels des agents, certaines sont sensibles : appartenance syndicale, certaines données médicales comme l'état de santé ;
- Les données utiles pour les demandes d'aide au logement en lien avec le handicap. Souvent les personnes exposent dans leur lettre de demande leur maladie et donc des données de santé : Ces données ne sont pas numérisées dans des progiciels spécifiques mais elles circulent par mails entre les agents et les C.T (communes, intercommunalités, envoi au département qui a la compétence sociale). Le format de ces informations est souvent sous forme scan et elles sont stockées sous format PDF et papier.

L'EHPAD d'une ville auditée est un EHPAD municipal, administré par un conseil d'administration du CCAS (Centre Communal d'Action Sociale). C'est le maire de la ville qui préside ce conseil d'administration. Les cadres, médecins et employés qui travaillent à l'EHPAD sont des employés salariés du CCAS. Ils ont le statut d'employés municipaux et à ce titre manipulent des données personnelles et sensibles en fonction de leur métier et de leurs responsabilités.

Un dossier individuel résident est numérisé. Il contient des informations personnelles et sensibles, une traçabilité quotidienne des traitements et des prescriptions est assurée, allant jusqu'aux ordonnances.

Dans une autre ville, l'EHPAD n'est pas municipal, il est géré par le directeur de l'établissement. Les données personnelles ne sont pas échangées entre l'EHPAD et la mairie de cette ville.

Les données personnelles considérées comme sensibles par les agents :

D'autres données sont considérées comme « sensibles » par les agents eux-mêmes et font l'objet d'une prudence certaine dans leur traitement même si elles ne tombent pas sous la définition légale d'une donnée sensible. Ce sont :

- Les données sociales qui rentrent dans l'intimité de la personne : famille d'accueil, parent ou fratrie en prison, addiction ;
- Dossier enfant avec une partie sociale : comportement inadapté ou violent, environnement radicalisé, addictions, trafic de drogues, victimes d'inceste ou de pédophilie.
    - Note : un CRPI « recueil d'informations préoccupantes » est transmis en cas de signalement au conseil départemental pour la protection de l'enfance. Ce CRPI peut être effectué par n'importe quel agent d'une collectivité s'il juge que l'enfant présente des troubles ou des signes préoccupants.
- Les infractions présentes dans le casier judiciaire. Le casier judiciaire ne rentre cependant pas dans la catégorie des données sensibles ;
- Les sanctions disciplinaires dans le cadre du travail ;

- L'indication « fiché S » ;
- Le mariage entre personnes d'un même sexe : si l'orientation sexuelle est une donnée sensible, le mariage homosexuel qui donne clairement une telle indication est quant à lui rendu public. Une telle indication n'est donc pas une donnée sensible.

Enfin, il convient de préciser que certaines données sont considérées comme secrètes par les C.T et conservées sans être communiquées le temps de la procédure de traitement. Par exemple l'instruction d'une demande de dossier d'urbanisme qui peut impliquer des enjeux financiers et de possibles pressions.

5) Certains fichiers des C.T n'ont pas de données personnelles

Plusieurs applications métiers gérées par les C.T ne contiennent pas de données personnelles directes. Par exemple sur une ville de grande taille, sur environ 200 applications métiers offrant des services aux citoyens, 110 seulement gèrent des données personnelles, dont 16 avec des données considérées comme sensibles (voir paragraphe « L'ensemble des fichiers des C.T avec données personnelles sensibles »).

La plupart du temps les informations de base sont les données individuelles telles que définies dans le paragraphe « classification des données personnelles ».

6) Synthèse des fichiers des C.T contenant des données personnelles

Ce paragraphe contient la synthèse des collectes de données effectuées auprès des C.T sollicitées dans cette étude.

Les données du recueil sont classées en fonction du domaine de compétences des C.T. *La liste des compétences des collectivités territoriales est disponible dans l'Annexe 3 dans le document « Tableau synthétique des compétences des collectivités territoriales françaises et de leurs groupements ».*

On trouve ainsi des données personnelles au sein des compétences générales suivantes des C.T :

Compétences communes à toutes les mairies :

- Action sociale, médico-sociale et solidarité
- Culture / Vie sociale / Jeunesse et sports / Loisirs
- Formation / Enseignements / Education
- État civil / Citoyenneté

Compétences spécifiques aux communautés de communes :

- Aménagement du territoire / Infrastructures et transports

Notons également que les CC selon la loi NOTRe peuvent également avoir des compétences optionnelles ou facultatives. C'est à l'appréciation des élus locaux. Par exemple la Jeunesse (subventions, participation à des accompagnements), les équipements culturels, etc.

Compétences communes à la fois aux mairies et aux communautés de communes :

- Gestion
- Logement et Habitat
- Sécurité

Au-delà des compétences, on trouve des fonctions qui soutiennent l'organisation et les usages des C.T :

Fonctions soutenant l'organisation et les usages des collectivités territoriales

- Communication
- Finances et taxation (si les données participent à l'élaboration des demandes de règlements financiers, les applications métiers ne vont pas jusqu'au paiement et le traitement financier bascule par la suite vers la direction financière et la trésorerie municipale)
- Ressources Humaines

7) L'ensemble des fichiers des C.T avec données personnelles sensibles

En se référant à la définition de ce qu'est une donnée sensible *« Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle* » (cf. paragraphe ci-dessus), effectuons un focus sur les données personnelles jugées sensibles utilisées par les C.T.

On y retrouve beaucoup de données de transit qui sont collectées et transmises par les C.T, mais qui ne sont pas traitées en interne. Elles concernent majoritairement les données liées à la santé des personnes. Dans le cadre des instructions d'aides sociales accordées aux personnes (qu'elles soient techniques ou financières), les communes collectent des informations privées sur les demandeurs. Celles-ci sont stockées la plupart du temps dans un dossier papier au service social des communes, puis transmises par mail à l'intercommunalité et parfois au Conseil départemental pour certaines aides. Les données de santé, de situations familiales, judicaires et autre circulent par mail, non cryptées, d'un agent d'une structure à l'autre.

Il est important de noter que les sauvegardes sont effectuées à chaque niveau de collectivité et que leur durée de conservation est à propre à chaque structure.

Les données sensibles vues par une ville moyenne :

Pour s'en tenir à la définition de la CNIL, seules les données de santé sont concernées.

Par conséquent, seul l'EHPAD de cette ville traite ce type de données, avec pour finalité de traitement la gestion des dossiers médicaux et des soins des résidents. Le nom de l'application utilisée est ASCLEPIOS de l'éditeur logiciel ALTAIR. Les données sont hébergées sur les serveurs de fichiers dans le « Datacenter » de la ville. Les données sont sauvegardées toutes les 15 minutes de manière automatique. La sauvegarde de données sensibles de l'établissement de santé dans le serveur de la commune est, à ce jour, non conforme. Une démarche de mise en conformité est en

cours pour faire héberger ces données en dehors de la collectivité sur un serveur labellisé à recevoir des données de santé.

Le nombre de déclarations simplifiées auprès de la Cnil par la ville est de 67. Sur ces 67, seules 3 sont des déclarations de données dites « sensibles ». Ces traitements concernent exclusivement les données de santé des résidents de l'EPHAD

Les données sensibles vues par la une ville de taille moyenne :

Domaine de collecte de données nominatives	**Traitement informatique et suivi par un logiciel métier dédié**	**Détails des données particulières autres que l'état civil**
Action sociale, médico-sociale et solidarité	Aides sociales légales et facultatives (en lien avec conseil départemental)	Données de situations familiales Données d'appréciations de difficultés sociales Données de ressources du foyer et d'allocations familiales
Action sociale, médico-sociale et solidarité	Gestion du dossier médical et du dossier de soins à l'EHPAD	Données de santé, Données de de numéros de sécurité Sociale (NIR)
Action sociale, médico-sociale et solidarité	EVALUATION ET SUIVI DES PERSONNES AGEES ET HANDICAPEES (ergothérapeutes)	Données d'identification bancaire Données de santé et d'handicap,
Action sociale, médico-sociale et solidarité	GESTION DES SERVICES DE SOINS A DOMICILE (infirmiers)	Données de santé Données de de numéros de sécurité Sociale (NIR)
Action sociale, médico-sociale et solidarité	Suivi médical des agents et prévention des risques professionnels	Données de santé
Formation / Enseignements / Education	Gestion et Facturation des crèches	Données d'identification bancaire Données de situations familiales Données de ressources du foyer et d'allocations familiales
Formation / Enseignements / Education	Inscription et services scolaires	Données d'identification bancaire Données de régime alimentaire Données de situations familiales Données de ressources du foyer et d'allocations familiales
Formation / Enseignements / Education	réussite éducative	Données de situations familiales
Finances et taxation	Analyse Fiscalité Locale (rôle impôts locaux)	Données de ressources du foyer et de patrimoine
Logement et Habitât	Lutte logement vacant	Données de de patrimoine
Sécurité	Missions de police municipale	Données d'infraction et de verbalisation
Sécurité	Procès-verbal électronique	Données d'infraction et de verbalisation

Sécurité	Conseil local de sécurité et fichier de suivi de délinquance	Données de délinquance
Sécurité	Vidéoprotection établissements et lieux publics	Enregistrement vidéo des caméras
Communication	PORTAIL CITOYEN DEM@T	Données d'identification bancaire (à venir) Données de ressources du foyer
Ressources humaines	Gestion des mains courantes de l'assistante sociale	Données de santé Données de situations familiales Données d'appréciations de difficultés sociales Données de ressources du foyer et d'allocations familiales Données de de numéros de sécurité Sociale (NIR)

Cependant certaines autres informations sensibles sont stockées notamment pour :

- la cantine scolaire : régime alimentaire, qui donne des indications sur la religion ou la santé de l'enfant ;
- Les données RH (syndicalisme, maladies, sanctions disciplinaires, casier judiciaire).

IV. Comment sont-elles traitées ?

1) Préambule

En préambule à ce chapitre, il apparait opportun de présenter ici les cyberattaques auxquelles ont été confrontées certaines des C.T qui ont servi de support pour cette étude, ainsi que de présenter synthétiquement les impacts de ces attaques.

Collectivité	**Cyber - attaque**	**Type d'attaque**	**Impacts court terme**	**Impacts long terme**
Une petite communauté de commune	oui	2016 : Ransomware Locky (zip attachés).	Les données ont été sauvées grâce au backup du Cloud. Á noter un défaçage en 2015 par l'état islamique.	Les données plus anciennes de la CC n'étaient pas sur le Cloud à cause du prix de stockage. quelques anciennes données non récupérables mais non utiles pour la plupart.

Une moyenne communauté de commune	non			
Une ville moyenne	oui	Locky le 25 février 2016	Les fichiers des cinq utilisateurs identifiés ont été cryptés, i.e: des centaines voire des milliers de fichiers.	Aucun impact pour les usagers et les applications des accueils et des services au public. Aucune incidence financière.
Une ville moyenne	non	ponctuellement à des « bots » dormant sont identifiés et neutralisés par les dispositifs de sécurité (mails spam)		
Une très petite commune	oui	Locky	5 mois de données perdues	Meilleure prise de conscience Amélioration du service par le prestataire
Une très petite commune	non	Les emails d'origine inconnue sont éliminés, pas de données via clef USB		
Une très petite commune	non	Une seule adresse principale pour les messages pour la mairie. Permet un filtrage drastique.		
Une très petite commune	oui	En 2016 : par cheval de Troie (fichier joint à un courriel).	La société informatique a dû bloquer la pollution et rétablir certains fichiers à partir de la sauvegarde (environ 4 heures de travail).	Aucun
Une petite commune	non			

2) Entre open Data et sécurité : le choix de la sécurité

Les collectivités territoriales seront de plus en plus sollicitées pour mettre une partie de leurs données à la disposition des citoyens ou des entreprises pour satisfaire une demande de transparence de plus en plus forte, démocratiser l'accès à ces informations, ainsi que de permettre

un contrôle de l'efficacité des politiques publiques par l'ensemble des administrés. L'utilisation de ces données pourrait aussi favoriser la création de nouveaux services innovants[6].

Mais d'un autre côté, il est demandé par le RGPD à ces mêmes collectivités une sécurisation et une protection des données personnelles dont elles sont dépositaires, ce qui fait qu'elles sont prises entre les impératifs contradictoires de l'open data et la sécurisation des données. A la fois l'État français pousse à ouvrir les données, mais en parallèle il demande une sécurisation et un contrôle total de ces données, sous peine de sanction, ce qui apparait comme paradoxal pour les C.T.

Focus : le choix d'une commune a été de faire une approche collective de l'open Data. Par exemple, l'accessibilité sur son territoire est réalisée en partenariat avec une université, des commerçants du centre-ville et des associations œuvrant autour du handicap.

Il semble en effet difficile pour cette ville de concilier les deux exigences décrites ci-dessus.

3) Les traitements possibles des données à caractère personnel par les C.T.

6 Sandrine Turgis, journée d'études « La transformation numérique pour les collectivités territoriales : quels enjeux de sécurité et quels accompagnements ? », Vannes le 1er décembre 2017, chaire Saint-Cyr / Sogeti / Thales.

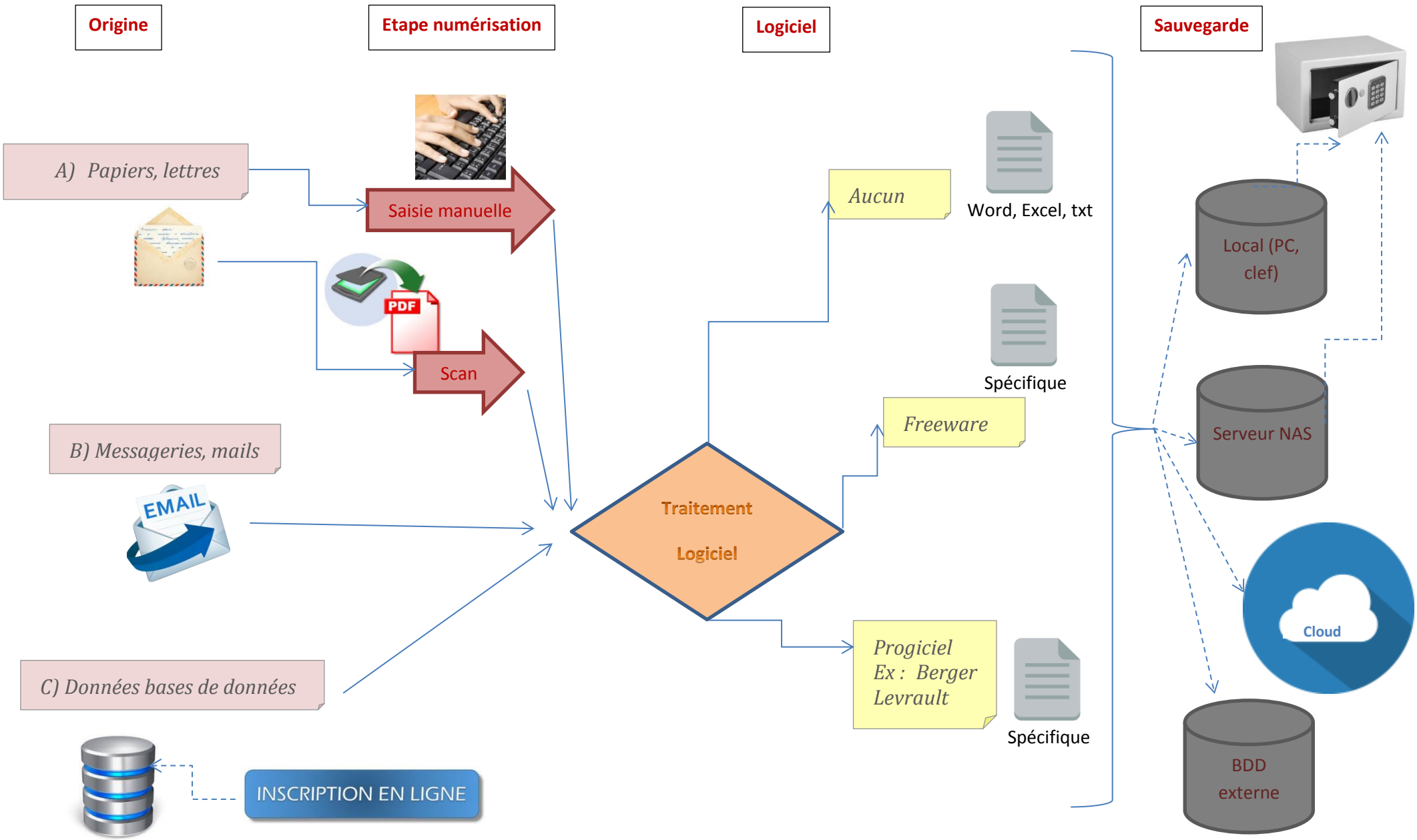


Schéma global listant les traitements possibles des données à caractère personnel par les collectivités territoriales

Les traitements des données personnelles par les C.T sont multiples. Sur ce schéma, on constate que toutes les configurations sont possibles, du traitement essentiellement papier à la dématérialisation de bout en bout.

Comme l'indique le schéma ci-dessus, les données peuvent être récupérées:

- oralement ;
- sous format papier, ce qui implique de les numériser :
    - soit a) de les scanner et de les conserver sous format PDF ou JPG ;
    - soit b) de les saisir dans un fichier type Word ou Excel ou .txt ;
    - soit c) de ne pas les numériser et de les conserver sous format papier, ce qui sort du cadre de cette étude.
- au sein d'un mail. Très souvent les mails ne sont pas détruits à l'issue mais conservés dans la messagerie. Les adresses mail sont fournies par les C.T ex : « mairie-xxx.fr, ville.fr, etc »
- via une interface numérique qui peut être au travers d'un portail numérique.

Les données personnelles numériques sont ensuite traitées par le service métier qui en a la responsabilité. Il existe trois types de traitement numérique :

- avec l'aide d'outils numériques simples tels que les logiciels les plus courants que sont Word, Excel et un éditeur de texte. Les fichiers ainsi créés servent de référence. Ils sont le plus souvent mis sur le réseau interne de la collectivité, mais sont parfois gardés sur le PC de la personne qui en a la gestion si elle est seule sur cette fonction.
- par des logiciels spécifiques réalisés pour la collectivité. Ce sont des logiciels Freeware dont seule la collectivité a usage. Ce cas semble de plus en plus rare, car les ressources nécessaires pour créer un logiciel Freeware ne sont pas accessibles par les C.T.
- par des progiciels du commerce développés par des fournisseurs de logiciels spécialisés. L'accès à ces progiciels se fait avec des contraintes de sécurité (login/password), et la maintenance est assurée par ces mêmes fournisseurs. Les données sont stockées dans les bases de données dédiées. Les bases de données de ces logiciels sont peu ou pas chiffrées, hormis celles contenant des données sensibles. Sur un même espace géographique, il est courant que les C.T utilisent le même progiciel.

Les données personnelles ne sont jamais chiffrées par les C.T, sauf à de rares exceptions et uniquement sur le Cloud. Le chiffrement est alors effectué par le prestataire fournisseur de la solution Cloud.

La sauvegarde des données personnelles est variable selon les choix des services qui en ont la responsabilité. Les données peuvent être sauvegardées :

- sur le PC de son utilisateur, hors réseau. Le plus souvent lorsque ce dernier utilise des données personnelles à des fins propres ;
- sur le serveur de la collectivité, comme le serveur local NAS (Network Attached Storage) ;

- au sein de bases de données propres au logiciel qui peuvent être déportées, ou bien stockées sur le serveur interne de la collectivité ;
- sur un serveur externe (tel que OVH) ;
- Dans un Cloud : certaines C.T utilisent en effet le Cloud pour sauvegarder leurs données. Les données peuvent être chiffrées sur le Cloud par le prestataire de service. Le niveau de sécurité du Cloud est généralement inconnu. Certaines villes demandent à ce que leurs données soient stockées en France par le prestataire.

La plupart des C.T assurent une double sauvegarde de leurs données en :

- Les stockant sur un disque dur qu'elles enferment dans un coffre-fort.
- Les dupliquant sur un Cloud.

Pour une autre commune approchée qui a décliné notre sollicitation en raison de l'étendue du travail de recensement des données et du manque de ressources humaines à y affecter, une réunion a permis de recueillir que le maire de cette commune conserve sur son PC plusieurs listes précises de personnes pour lesquelles la mairie est sollicitée pour des aides sociales ou qui ont des impayés à cause de situations familiales ou financières difficiles. Il en est de même pour les entreprises de la ville où ces fichiers aident pour l'aide à la diffusion. Seul le maire gère ces données qui sont sauvegardées sous un format Word ou Excel soit sur PC local, soit sur clef USB pour être rapportées à la maison. Elles ne sont pas chiffrées.

5) Le partage des données

Il existe de nombreuses formes de partenariats et d'échanges de données :

- ✓ En interne, d'agent à agent, c'est le plus souvent par mail. De logiciel à logiciel, cela est bien entendu propre à l'application mais s'effectue par échange automatisé sécurisé au sein du progiciel, ou bien par les fonctions d'export/import via une plateforme d'échange et authentification.
- ✓ En externe, les échanges s'effectuent le plus souvent dans les co-constructions d'un dossier individuel partagé par la ville avec un autre organisme.
- ✓ La dématérialisation inter-administration occasionne des échanges de données nominatifs au travers d'Internet et de fichiers structurés (Trésor-Public pour les dépenses/recettes, CAF pour les éléments sociaux, Préfecture pour le contrôle de légalité, ANTS « Agence Nationale pour les Titre Sécurisés » pour la verbalisation….). Le tout cadré sous convention et avec des moyens techniques individualisés et déterminés à l'avance.

Mais le plus souvent pour les communes de moindre taille, les échanges de données sont le fruit d'un usage qui est à l'appréciation des agents et des responsables.

Le partage des données sensibles est indispensable pour le suivi de la personne par les services des collectivités locales, voire les services de l'État (ex : cas d'un enfant dont le comportement scolaire est perturbé et qui doit être suivi par plusieurs acteurs : institutrice, assistance sociale, mairie, etc.).

Actuellement chaque service constitue son propre dossier, à partir des déclarations de son responsable légal ainsi que des professionnels qui suivent la personne concernée. L'inconvénient de ce système est la multiplication des fichiers et des procédures de déclaration par les personnes concernées, la non-concordance possible des données entre les différentes déclarations, un niveau de sécurité différent dû aux multiples acteurs qui ont chacun des réflexes de sécurité propres. Les professionnels ont des méthodes de travail et des obligations légales différentes (ex : assistantes sociales et institutrices). Or une bonne prise en charge de la personne supposerait un « secret partagé » à partir d'un dossier unique et confidentiel, qui permettrait une déclaration unique, une centralisation des données, une sécurisation et des accès personnalisés par type d'acteurs.

La numérisation constitue sur cet aspect une opportunité.

6) Synthèse globale des mesures techniques prises par les C.T

Pour les C.T que nous avons sollicitées, d'une façon générale il existe peu de mesures clairement identifiées par une politique de sécurité informatique.

Pour les plus petites C.T, ce sont souvent des personnes clefs qui assurent la dynamique de la sécurité de l'accès aux données.

Le plus souvent ce sont les postes de travail qui sont sécurisés par un login/password qui protège l'accès aux données.

L'accès à un progiciel se fait généralement avec des logins/password propres au logiciel. Seuls en ont connaissance les personnes habilitées à l'utiliser, c'est-à-dire les personnes d'un même service et leur supérieur. Les droits d'accès sont à l'appréciation du chef de service : cette politique de droit est donc une décision en interne, qui n'est le plus souvent pas décrite formellement.

Certains progiciels ont des fonctions qui ne sont accessibles qu'à certaines personnes ou à des supérieurs.

Une mairie a une politique très simple, mais jusqu'à présent efficace, de sécurité des données. Elle refuse systématiquement les clefs USB que les personnes leur apportent. En outre, tout email d'origine inconnue ou douteuse est détruit. Elle n'a jusqu'à présent pas subi de cyberattaques.

Autres exemples :

- au sein de certaines C.T, on rentre son password le matin sur sa station de travail, et on ne termine sa session que le soir. L'activation de l'écran de veille n'est pas toujours automatique.
- Pour une C.T, il existe un mot de passe pour une application métier et seuls les agents autorisés connaissent ce mot de passe. La directrice de l'application a de son côté des droits différents.
- Pour une autre C.T, il n'existe pas de hiérarchie entre les utilisateurs d'une application.
- Pour une autre encore, chaque agent a son propre mot de passe pour un accès à une fonction d'un progiciel. Ce qui permet la traçabilité des opérations effectuées (on sait ainsi quel utilisateur a fait quoi).
- Il existe aussi des C.T ou les comptes d'accès à des logiciels sont échangés par tous. Par exemple le même compte Google permet de se connecter de n'importe quelle station de travail.

a) L'externalisation : le cas le plus simple

Toute collectivité territoriale s'appuie sur des prestataires informatiques extérieurs, plus ou moins selon les moyens qui sont les siens.

Ces prestataires préconisent l'infrastructure et assurent le stockage des données.

Ces prestations passent par des contrats, mais bien souvent il est difficile pour les C.T de s'assurer de la pertinence technique et financière de la prestation, ainsi que des garanties !

De plus, dans les petites communes il n'y a pas de service juridique. La confiance est donc par défaut.

Les données sont saisies sur des progiciels métiers. Les C.T n'ayant pas les ressources humaines ou les expertises nécessaires font donc confiance aux prestataires, ce qui *de facto* déporte leur responsabilité. Ces externalisations sont par conséquent une solution de sécurité mais attention à la dépendance. Il faut assurer des contrôles de la conformité, ce qui ne semble être que très rarement le cas. Le risque en effet réside dans le fait que le propriétaire des données n'est pas le fournisseur, mais la collectivité.

Encart : contrat d'externalisation de la sauvegarde des données d'une petite C.T

Il est stipulé dans le contrat « une supervision régulière de la réalisation de vos sauvegardes ».

Au regard de cette clause, l'entreprise X était clairement en faute lorsque l'attaque par le virus Locky a chiffré toutes les données de la mairie, données qui n'ont pu être restituées par l'entreprise X car le serveur de sauvegarde n'était pas suffisamment dimensionné pour sauvegarder l'accumulation régulière des données de la mairie.

La mairie a fait confiance… et n'a pas porté d'action en justice contre X. Elle continue même de travailler avec eux !

b) La collectivité fait soi-même

En fonction des besoins exprimés par certains services, les C.T trouvent parfois en interne les compétences techniques ou les services support pour le développement d'outils spécifiques.

Il est très difficile de les lister car ces outils sont extrêmement variés, mais ne s'appliquent qu'à des applications non partagées avec d'autres services, à des usages ou habitudes internes, ou à des applications spécifiques à la collectivité.

L'utilisation de ces outils nécessite néanmoins des mesures de gouvernance qu'il faut clairement définir : accès, droits d'accès, suivi et mises à jour notamment.

Citons comme exemple les portails citoyens pour faciliter les liens avec les personnes. Ces portails sont des plateformes d'accueil numérique pour des activités de saisie en ligne et d'échange avec les citoyens : cantine, alsh, associations (demande de subventions), etc.

c) La conservation des données

Le bilan de tous les entretiens réalisés dans le cadre de l'étude pour le CREOGN est sans appel : les DGS ou les élus ne connaissent pas les règles de conservation des données à caractère personnel.

Les prestataires extérieurs, avec qui ils travaillent tous, ne les informent pas sur ce point et ne leur précisent pas la durée de conservation des données qu'ils leur confient, ni le lieu où ces données sont conservées.

Les personnes interviewées ne savent pas à qui demander cette information. Ils s'en remettent en toute confiance à leur prestataire. Par ailleurs, par sécurité, les petites communes, mais également les plus grandes, archivent les documents en papier dans des placards dans les bureaux. Ils préfèrent tout conserver par sécurité et assurer, en cas de perte informatique, la continuité du service. Le principe de précaution est très fort dans les collectivités territoriales. Ils font totalement confiance aux prestataires informatiques à qui ils confient leurs données, mais ils « assurent » en conservant un format papier au cas où !

Il est à noter que parfois les DGS effectuent des sauvegardes personnelles de données sur disques durs externes. Si généralement les disques durs sont stockés dans des coffres-forts dans la mairie, certains les rapportent chez eux.

d) Les mesures organisationnelles prises aujourd'hui par les C.T

L'organisation des collectivités territoriales pour la gestion (stockage et protection) des données à caractères personnel est la plupart du temps liée à l'histoire et aux modes de fonctionnement propres à chacune d'entre elles.

Il n'existe pas de préconisations ou de règles imposées aux C.T sur les mesures organisationnelles. Chaque commune est maîtresse chez elle.

De ce fait, la gestion des données collectées par la collectivité suit la même organisation de stockage des données que pour les dossiers papier avec quelques règles cependant : un stockage dans la mairie (le serveur s'y trouve la plupart du temps), des sauvegardes par métier et par direction, un double archivage (papier et numérique) avec une préférence pour le papier pour les petites communes. Un DGS estime que 80 % des données collectées par les petites mairies sont archivées dans des dossiers papier, puis dans une salle d'archivage (souvent au grenier de la mairie avec des accès non contrôlés ou limités)

L'introduction des outils numériques dans les métiers des agents des C.T étant antérieure à la gestion et au stockage des données des citoyens, les politiques en la matière ont naturellement suivi les us et coutumes appliqués depuis des décennies et n'ont pas été nécessairement formalisées par le DGS auprès des agents de sa collectivité.

Le sentiment général qui émerge dans une C.T est que la donnée collectée appartient au service qui la collecte ou qui l'exploite. Il en a la responsabilité et en assure, de fait, la bonne conservation. C'est une appréciation toute personnelle de l'agent ou du chef de service. La notion de praticité est également notable, c'est-à-dire de pouvoir retrouver en toute circonstance une information et rapidement, si possible. Un DGS avoue ne pas utiliser du tout le réseau interne de la commune dont l'arborescence a été mise en œuvre par les techniciens informatiques, tant elle est complexe et difficile. Ceci génère une perte de temps qu'il ne souhaite pas perdre. Il a donc créé son propre fichier « personnel/professionnel » sur son poste de travail.

Tous les responsables de C.T avouent ne pas maîtriser à 100 % les fichiers des agents contenant des données à caractère personnel, voire sensibles, même les villes moyennes qui gèrent près de 200 applications métiers. Le manque d'information et la priorité accordée aux aspects pratiques (facile et rapide) provoque la naissance de fichiers hors réseaux, construits par les utilisateurs. Ces fichiers peuvent échapper totalement au contrôle des DSI ou des DGS.

L'arrivée du numérique dans les usages des C.T n'a pas été accompagnée de l'application de bonnes pratiques ou de la mise en œuvre d'une politique numérique applicable par tous.

La politique de protection et de stockage des données dépend de la volonté du dirigeant et de son appétence pour ces sujets. Pour une petite commune, sachant que les équipes d'élus sont très resserrées et ont en charge de multiples portefeuilles (sans obligatoirement les connaissances qui devraient les accompagner), c'est de la sensibilité du DGS que dépend la politique numérique de protection. Le seul garde-fou ou opérateur de régulation est actuellement la CNIL. Mais leur mode de fonctionnement a ses limites :

- La CNIL est perçue comme répressive et non dans l'accompagnement. Les C.T ne les sollicitent donc pas afin de ne pas inciter à la curiosité et provoquer des contrôles ;
- Ses effectifs réduits en France semblent les empêcher de remplir cette mission de contact direct avec les C.T.

Les C.T informées de leurs obligations en matière de sécurité et protection des informations et des données à caractère personnel (DGS et DSI) le sont principalement via les réseaux auxquels elles appartiennent (AMF, associations nationales de C.T de leur taille, Centre de gestion, syndicats professionnels, …) ou encore par les supports de communication qui leur sont réservés (la gazette des communes, …). A minima, elles savent, pour avoir eu connaissance de problèmes dans certaines communes ou intercommunalité, qu'ils doivent effectuer des « *déclarations simplifiées* » auprès de la CNIL pour des usages de données personnelles au sein de leur organisation. La problématique est différente pour les communes moyennes ou grandes. Elles sont mieux informées car mieux structurées et dotées.

Il est à noter également qu'il est difficile parfois d'obtenir des informations des différents services sur leurs méthodes de travail en matière de gestion et de protection des données à caractère personnel. Ex : 2 DGS interviewés avouaient ne pas avoir eu de retour des quelques services sur les questions demandées. Le sentiment d'intrusion dans un mode de fonctionnement provoque des blocages de la part de certains agents, voire même de rétention d'informations. Les autres motifs sont également la peur du jugement, la peur des modifications de pratique que cela pourrait entrainer, l'instinct de protection des données ou informations qu'ils gèrent.

Une commune pratique une double sauvegarde de 80 % des données des citoyens ou de données publiques : l'archivage papier et la sauvegarde numérique. En ce qui concerne les dossiers papiers, ils sont tous stockés au grenier de la mairie depuis des décennies sans distinction de sujet ou de finalité métier. Il n'y a pas de restriction d'accès sauf la demande effectuée auprès du DGS pour y accéder. Après accord, l'accès est libre et non accompagné.

Le site n'est pas sécurisé spécifiquement par des portes renforcées, des codes ou autre outil spécifique. En cas d'accident (incendie, inondation, …) les dossiers pourraient être partiellement détruits.

Pour l'archivage numérique, il est sous-traité à un prestataire extérieur dans le serveur de la collectivité, situé dans la cave aménagée de la mairie. L'accès s'effectue par l'extérieur par une porte blindée avec clé et qui donne sur un parking public (accès de l'extérieur très aisé).

V. Les recommandations proposées

Les recommandations suivantes ne sont pas exhaustives, mais sont liées aux constatations de ce qui a été observé sur le terrain.

Elles sont issues d'échanges avec les élus et les agents sur le terrain qui nous ont exprimé leur vécu et ressenti de la façon dont une C.T peut gérer des données personnelles, ainsi que des constats des auteurs de ce rapport.

1) La gouvernance globale

Le Règlement général sur la protection des données (RGPD) devrait modifier substantiellement le fonctionnement actuel sur un certain nombre de points.

Il précise le champ d'application territorial du Règlement et y inclut les activités dirigées vers l'Union européenne par les responsables de traitement implantés dans des pays tiers. Il substitue très largement le régime de l'auto-certification à celui de l'autorisation préalable, le responsable du traitement devenant le premier garant de la protection des données.

Mais, sur le fond, le RGPD ne modifie pas l'esprit ou la lettre du dispositif existant. La mention des données génétiques ou biométriques ne fait que confirmer la jurisprudence antérieure en ce sens que les empreintes digitales ou la reconnaissance faciale aussi bien que la séquence ADN sont effectivement de nature à permettre l'identification d'une personne. Ce règlement sera directement applicable à partir du 25 mai 2018.

Ce rapport ne propose pas un seul modèle de gouvernance pour répondre aux exigences de la RGPD, mais il décline plusieurs solutions possibles en fonction de la taille et des compétences des acteurs.

a) S'appuyer sur les structures existantes et renforcer leur expertises et moyens

Partant des postulats précédents, et pour envisager des recommandations, il est indispensable d'intégrer fortement l'accompagnement à la conduite du changement auprès des agents. Les agents sont ceux qui produisent de la donnée à caractère personnel et leur adhésion est nécessaire.

Si la défaillance humaine représente le facteur de risque le plus fort dans les organisations en ce qui concerne les risques de cyberattaques, il en est de même sur la mise en œuvre d'une politique de protection des données à caractère personnel efficace.

Pour cela, il semble opportun de réfléchir à des points en priorité :

1) proposer aux C.T une organisation capable de les accompagner dans ces changements de pratiques ;
2) accompagner et expliquer la mise en œuvre de ces pratiques protectrices des données aux agents des collectivités territoriales.

Quelle organisation peut être envisagée ?

Il semble judicieux et pertinent de s'appuyer sur des structures existantes ou des expériences territoriales efficaces, ayant fait leurs preuves.

La CNIL n'est pas perçue par les C.T comme un partenaire et un accompagnateur par les structures.

Il est nécessaire pour les C.T de prévoir une organisation resserrée, visible et compréhensible, et enfin légitime (une culture incontestable des TIC).

3 niveaux d'intervention seraient possibles :

A – **Au niveau national** : l'organisation de référence serait rattachée au 1er Ministre et bénéficierait d'un champ d'actions interministériel. Ce postulat apporte de la crédibilité et place le sujet au niveau de priorité nationale. La seconde possibilité est un rattachement au Ministère de l'Intérieur, justifié par le fait que la Police et la Gendarmerie nationale œuvrent déjà au quotidien sur le territoire sur le thème Cyber (sensibilisation, attaques cyber, …).

Une structure telle que l'ANSSI répond à ces critères, même si ses effectifs en Région ne sont à ce jour pas adaptés aux besoins. La notion d'organisation nationale de référence, clairement affichée par le gouvernement, est très importante. Elle positionne le sujet et annonce les missions, les cibles, les moyens mis en œuvre. Il s'agit d'un partenaire de confiance.

B – **Au niveau régional** : il s'agit de la seconde porte d'entrée sur le sujet de la protection des données à caractère personnel dans les C.T. Elle peut s'apparenter à une sorte de guichet unique. Il doit être clairement identifié également, être une structure indépendante, bien intégrée sur le territoire régional.

Pourquoi cette structure doit-elle être indépendante ? Parce que son intégration dans une structure politique du type conseil régional ou conseil départemental provoquera des réticences de certaines C.T. Ce sont des structures trop connotées politiques ou au fonctionnement « administratif ou technocratique ».

Pour la bonne intégration, il faut comprendre ici, une légitimité sur le positionnement des sujets numériques, accompagnement des C.T ou encore connaissance de l'environnement. En Bretagne par exemple, Mégalis Bretagne pourrait remplir cette fonction (www.megalisbretagne.org).

Ce syndicat mixte financé par les C.T bretonnes de toutes tailles est basé à Rennes et sa mission est de mutualiser le déploiement de la fibre optique sur l'ensemble de la Région en concertation avec les départements et les intercommunalités, mais également d'accompagner les C.T dans les usages du numérique et la modernisation de l'administration publique. Il s'agit ici des dossiers tels que l'archivage numérique, la dématérialisation des marchés publics, la dématérialisation de la chaine comptable. Mégalis assure déjà depuis plusieurs mois également la sensibilisation et l'information des C.T au RGPD et au DPO via des tutoriels mis en ligne et des réunions de formation.

Dans notre sujet, il s'agit d'imaginer une structure (existante ou à créer) qui assurera l'accompagnement de la mise en conformité du stockage et de la protection des données des organisations territoriales.

Les missions de la structure régionale seraient alors :

- La formation des agents,
- L'information des obligations des élus et des dirigeants,
- Les préconisations d'organisation interne et de gouvernance,
- La mutualisation d'un DPO au service des C.T en fonction des compétences obligatoires des structures et de la taille des communes ou intercommunalités,
- La mise à disposition des relais sur les territoires d'un « kit clé en main » sur les bases de mise en œuvre d'une politique de sécurité numérique : simple et facile à mettre en œuvre,
- Une liste des prestataires informatiques labellisés par la structure de référence nationale, par territoire géographique,
- Etc.

C- **Au niveau des territoires** : l'intercommunalité semble l'échelon le plus pertinent pour diffuser les politiques de protection des données à caractère personnel et de sécurisation des systèmes d'informations.

Quelques points de vigilance sont à soulever cependant :

Les intercommunalités sur ce sujet sont plus en retard que de nombreuses communes de taille moyenne et grande. Ceci est dû au fait que celles-ci ne manipulent pas autant de données à caractère personnel. Par ailleurs, les intercommunalités ne sont pas pourvues de structures informatiques fortes. Leurs effectifs peuvent se limiter à 2 ou 3 personnes quand pour une ville moyenne ils peuvent aller jusqu'à 20 personnes. Ce sont la plupart du temps des techniciens qui ont en charge l'infrastructure réseau ou le suivi du déploiement du réseau FTTH (Fiber To The Home).

Il faut noter également que de nombreuses intercommunalités ne se sont pas encore préoccupées du RGPD ou de l'obligation de disposer d'un DPO en mai 2018. La loi NOTRe a profondément modifié les organisations territoriales en opérant des fusions. Celles-ci ont modifié leurs champs d'actions et leur ont pris beaucoup de mobilisation en temps et en énergie sur de multiples chantiers. La sécurité numérique et la gestion des données à caractère personnel ne sont pas pour elles une priorité.

Pourquoi dans ce cas, pourrait-on confier ce sujet aux intercommunalités ?

- Elles regroupent de nombreuses communes de toutes tailles ;
- Elles sont entendues et écoutées par ces dernières. Une de leurs missions est d'être au service du territoire et des besoins des communes membres ;
- Elles souffrent moins des réductions budgétaires et sont soucieuses de répondre aux attentes de leurs membres ;
- Le socle des données à caractère personnel est commun pour toutes les communes puisqu'il dépend fortement des compétences obligatoires *(cf. le tableau des compétences Annexe 1).* Certaines sont développées commune par commune, mais un DPO mutualisé à cet échelon territorial pourra gérer les spécificités ;
- La philosophie des intercommunalités est la mutualisation des ressources (y compris financières) au service de tous. Exemple de mutualisation : une intercommunalité propose à chaque commune membre de bénéficier, moyennant participation financière, du serveur de stockage des données toutes les nuits.

D'autres options pour les villes de plus grande taille :

Pour les communes plus grandes, il est intéressant également de leur proposer de la souplesse en leur permettant de s'organiser par leurs propres moyens, et ce pour plusieurs raisons.

- La première est que souvent, elles sont mieux pourvues en structures informatiques que leur propre agglomération. Elles sont donc en avance et ont réfléchi, via leur réseau de DSI aux mesures à prendre, au moins sur les aspects techniques et de gouvernance.
- La seconde est liée aux usages mêmes. Les villes plus grandes ont un nombre d'applications métiers beaucoup plus important qui rendrait le travail du DPO mutualisé au sein de l'intercommunalité beaucoup trop lourd. Il y passerait beaucoup trop de temps, sachant que les besoins sont surtout ressentis dans les plus petites communes.
- Enfin, les villes de taille plus grande sont généralement accompagnées par des prestataires informatiques extérieurs qui assurent la conservation, le stockage et la protection des données. Ce sont des critères définis dans les contrats de prestations.

Une autre option : les CDG

Si l'échelon de l'intercommunalité n'est pas jugé pertinent, d'autres pistes se dégagent sinon sur les territoires. Il est préconisé que ce soit des structures qui travaillent au quotidien avec les collectivités territoriales. Ex : les centres de gestion.
Un CDG vient de lancer le recrutement d'un DPO au sein de sa structure. Sa mission sera d'accompagner les communes qui le souhaitent sur leur mise en conformité avec le RGPD.

Reste cependant en suspens la question de l'accompagnement aux modifications d'organisation interne de gestion des données à caractère personnel et à la sensibilisation des agents aux bonnes pratiques. Ce sujet reste une priorité à intégrer dans des propositions d'accompagnement aux communes.

Recommandations :

- Trois niveaux sont envisageables (national, régional et intercommunal) et se doivent de se saisir de la question et proposer un plan d'action, des feuilles de route en lien direct avec les C.T et décliné selon leur particularité : réunions de travail, audits, conseils etc.

b) Relations collectivités locales et prestataires extérieurs :

Le cas de l'attaque par Locky sur une petite commune et les pertes de données consécutives qui en ont suivi montre l'urgence d'aider les C.T à gérer leurs relations contractuelles avec des prestataires extérieurs.

Recommandations :

- La création d'un guide de bonnes pratiques pour les collectivités territoriales, par l'ANSSI.
- La formation des agents et des prestataires extérieurs. La formation porterait sur la responsabilité qu'ont les C.T sur les données personnelles qu'elles gèrent, ainsi que sur les négociations et exigences à avoir sur les contrats avec les prestataires extérieurs.
- Une labellisation des certifications qui peuvent être accordées aux prestataires extérieurs.
- Il pourrait également être intéressant d'éditer un guide des critères à valider dans le choix d'un prestataire extérieur. Ce guide serait utile aux petites communes comme aux grandes !

2) Les politiques à mettre en œuvre

a) Les moyens techniques à mettre en œuvre :

Il faut adapter les moyens techniques en fonction des ressources qu'ont les C.T. Il ne sera en effet pas possible d'imposer une solution technique identique et globale pour les C.T qui n'auront pas les moyens de les mettre en œuvre.

Il faut néanmoins se conformer aux préconisations existantes.

Les C.T doivent par conséquent conserver les moyens de contrôler les prestations effectuées par les prestataires extérieurs. L'ANSSI étant le référent conseil pour les moyens à mettre en œuvre, il faut pour cela qu'il informe les C.T sur les points clefs techniques à exiger et à contrôler en cas de prestation extérieure.

Il est à notre sens important de porter un effort particulier sur les points suivants :

Recommandations :

- Préciser les moyens de chiffrement possibles et accessibles pour les C.T ;
- Préciser les moyens de duplication et de sauvegarde, et les avantages et inconvénients de chaque solution.

b) La formation des personnels :

Il est obligatoire pour la mairie de protéger les informations personnelles de chaque citoyen et de les réserver à l'usage pour lequel elles leur ont été confiées. Ces données sont non diffusables, ce qui nécessite donc une sensibilisation et une formation des personnels.

Le DPO pourrait lui-même assurer une fonction de formation des agents, mais son temps risque d'être contraint donc il faut envisager d'autres manières de former les agents : le Centre National de la Fonction Publique Territoriale (CNFPT), le Centre De Gestion (CDG), les ressources Humaines (RH) en interne, les centres de formation spécialisés sont des pistes à étudier.

La formation passe aussi par une pratique régulière et renouvelée d'exercices de gestion de crise cyber, permettant au personnel de se tester et de prendre connaissance de ses faiblesses et d'adapter ses comportements et processus en matière de cybersécurité.

Recommandations :

- Il est suggéré que l'échelon régional s'empare de ce sujet et propose des exercices de simulation d'attaques et de gestion des crises. L'échelon régional est à privilégier car il évite toute tension ou incompréhension qui pourrait avoir lieu à un échelon plus local.

c) Politique de protection des données

Sur une petite commune ayant subi une attaque en février 2016 par le virus LOCKY, impliquant 6 mois de données perdues et non récupérées.

L'attaque subie par la commune a choqué fortement les agents. Divers sentiments les ont traversés : l'humiliation de s'être fait piéger, la remise en cause de leur compétence et de leur sens des responsabilités, la peur des usages malveillants des données volées et plus que tout la culpabilité.

L'effet positif de cette attaque a été un changement radical des pratiques au sein de la mairie, mais aussi des comportements de tous les agents. Cette aventure collective a soudé les agents dans leur responsabilité commune de protéger leur bien : les données de leurs concitoyens. Dorénavant, ils communiquent davantage entre eux et dans le cas d'un doute sur un mail malveillant, ils consultent un collègue, voire même la DGS ou le Maire, avant de cliquer.

Cette attaque a eu pour effet de faire prendre conscience des risques et les systèmes de protection sur les postes et les serveurs ont été renforcés. La triple sauvegarde est désormais de vigueur dans cette mairie depuis l'incident.
Règle : Si l'on est victime d'une attaque cyber, on réagit immédiatement pour limiter les risques et on modifie son comportement !

Quelques Recommandations :

- Faire en sorte de ne pas attendre l'attaque et le drame pour réagir. L'utilisation d'exemples concrets de ce type est très pédagogique et marquant pour les élus. L'objectif est de motiver les décideurs à réagir.

- Nécessité de faire monter cette prise de conscience et cette responsabilité au plus haut niveau de l'organisation. Maintenir ce sujet au niveau des techniciens n'est pas efficace car ceci déresponsabilise les décideurs. Cette ambition permet aux dirigeants de prendre leurs responsabilités et mettre en œuvre les moyens humains, financiers et techniques pour pallier les risques. Il faut rappeler aux maires et aux DGS que ce sont eux qui portent les risques juridiques et financiers.

- Aller plus loin dans la responsabilisation des décideurs en leur faisant signer une lettre d'engagement. A cet effet la ville de Vannes a fait signer un tel document au Maire et au DGS : *voir l'annexe 2 « lettre d'engagement pour la protection de l'information de la ville de Vannes ».*
  Les C.T ne connaissent pas le RGPD et son contenu. C'est avant tout un règlement dont l'objectif est de protéger le citoyen. Ils le voient comme une contrainte supplémentaire pour eux. Cette règlementation est incomprise. La présentation du RGPD sous l'angle du citoyen les informe de leurs devoirs vis-à-vis du droit à la protection des données des citoyens. Les conséquences d'un non-respect de la règlementation peuvent également être dramatiques en terme d'image avec à la clé une perte de confiance de leur population.

- Miser sur l'humain et accompagner les C.T à sensibiliser leurs agents aux bonnes pratiques. Ex : une ville a décidé de former tous ses agents à la protection des données à caractère personnel et aux bonnes pratiques numériques. 8 sessions de 3 heures, obligatoires, même aux personnes ne travaillant pas sur un poste informatique. Cette sensibilisation rentrait dans le décompte des temps de formation des agents. Le message était : « la protection des données à caractère personnel et la sécurité numérique, c'est l'affaire de tous ! ».

Il est important également de déculpabiliser les agents et de les accompagner en cas d'attaque cyber. Les traumatismes sont réels et le suivi parfois nécessaire : « Cela peut arriver à tout le monde ».

- Inciter les C.T à se mettre en conformité avec ce qui existe déjà : le Référentiel Général de Sécurité (RGS), la charte informatique, le guide des bonnes pratiques de l'ANSSI et de la CNIL.

d) Politique de conservation des données

Les mairies sont donc de véritables coffres forts de données publiques, de données à caractère personnel, tout autant que de données sensibles qu'elles conservent sans limite de durée.

Recommandations :

- Il faudrait une politique effective de conservation des données dans le temps car elles ne sont pas toujours existantes dans les C.T, ni même pour les formats papiers. Il serait important également de faire appliquer rapidement et partout les politiques, règles et recommandations existantes.
- Il faut définir qui, au sein des C.T, est en charge de la destruction de ces données.
- Une application des règles implique une destruction des fichiers papier ou numériques (emails) une fois que les données ont été saisies dans le progiciel ou le fichier métier qui les centralise.
- Mais quelle protection des données papier (vol, protection contre la destruction) ? La loi impose de ne pas conserver les données personnelles. Mais il y a un dilemme entre conservation du patrimoine historique de la commune et la protection des données à caractère personnel de chacun. La solution devrait venir des règles concernant l'archivage. Les auteurs **préconisent une étude sur ce point particulier** (avec DPO et archivistes) pour déterminer à partir de quand et comment une donnée devient historique.

e) Faire évoluer la culture et l'organisation des collectivités locales en matière de traitement des données personnelles.

Les collectivités locales ont une longue expérience de la gestion des données publiques et ce serait leur faire un mauvais procès que de les accuser de ne s'être jamais souciées jusqu'à la mise en œuvre du RGPD de la nécessité de protéger les données personnelles relatives aux administrés. Mais, ce règlement introduit une nouvelle philosophie de la gestion des données. Il pose le risque d'atteinte aux données personnelles au cœur du raisonnement, supprime le contrôle a priori des traitements au profit d'une responsabilisation des élus et entend renforcer les droits des personnes sur les traitements de données les concernant. Incontestablement, le RGPD veut donner à la fois plus de liberté aux responsables des traitements mais sous le contrôle des personnes concernées et avec une possible mise en cause de leur responsabilité en cas de difficulté. C'est cette nouvelle philosophie, qui rompt clairement avec la culture française d'administrés soumis à des collectivités bienveillantes

qu'il convient de mettre en œuvre à travers la réorganisation des processus internes de gestion des différents services.

Recommandations :

Cette réorganisation doit être conduite avec pour principes directeurs :

- La frugalité : profitant des progrès techniques, les acteurs publics et privés sont friands de données personnelles et de traitements supposés nourrir leur réflexion et leur action. Les perspectives offertes par le « Big Data » et les objets connectés laissent augurer une boulimie de ces données dans les années à venir. Les collectivités locales qui se laisseraient aller à cette tendance doivent bien en mesurer les conséquences en termes d'obligations à satisfaire pour se mettre en conformité avec le règlement européen. Le filtre du contrôle préalable ayant disparu, c'est sous leur responsabilité que la collecte et le traitement des données seront conduits. Elles seraient bien inspirées de se montrer prudentes face à la « tentation technologique » et aux multiples offres qui leur seront faites de se doter d'outils plus ou moins invasifs qui ne manqueront pas de fleurir très prochainement. La mise en œuvre du RGPD est sans doute une bonne occasion de s'interroger sur la nécessité de tel ou tel traitement ou, au sein de tel traitement de la collecte de telles ou telles données. La frugalité pourrait s'avérer un principe utile pour limiter les risques d'atteinte et la mise en cause des responsables du traitement.

- La protection : même si elles s'astreignent au principe de frugalité, les collectivités locales devront mettre en œuvre un nombre significatif de traitements impliquant le recueil et l'utilisation de données personnelles, voire de données sensibles. Il leur revient alors de se réorganiser pour leur assurer le niveau de protection adéquat, un niveau élevé de protection étant requis pour les données sensibles. Cette réorganisation passe par deux types d'action : sur les processus et sur les personnes.
    - Les processus doivent être conçus dès l'origine pour protéger les données recueillies contre les risques d'atteinte qui peuvent conduire à leur captation, leur déformation, leur perte… Des audits devront être conduits pour vérifier que la sécurité est garantie tout au long de la chaîne du traitement, y compris pour la partie de cette chaîne qui est confiée à des prestataires extérieurs.
    - Concernant les personnes, élus et agents des collectivités locales, celles-ci devront être formées pour que l'importance nouvelle de la donnée personnelle soit prise en compte et que sa protection fasse l'objet d'un soin renforcé lorsque celui-ci est nécessaire. Il ne s'agit pas de dire que les élus et agents des collectivités locales ne portaient jusqu'ici aucune attention à la confidentialité des informations personnelles recueillies par leurs services et que ces informations étaient laissées à la libre disposition de tout un chacun. Mais, les avancées technologiques induisant un appétit croissant pour les données, les gisements de données détenues par les collectivités locales ont vocation à devenir des objets de convoitise particulièrement attirants.

- La transparence : les personnes concernées par les données personnelles qui font l'objet d'un traitement au sein des collectivités locales disposent déjà de longue date de droits qui

ne sont pas substantiellement modifiés par le RGPD sur le fond. Elles peuvent en demander la communication, en exiger la rectification si elles sont erronées… Mais, ici encore, le RGPD instaure un nouvel esprit visant à instaurer une obligation de transparence renforcée de la part des responsables de traitements. Les collectivités locales devront donc prévoir de renforcer le caractère explicite et formel des procédures permettant aux administrés d'être informés et d'exercer leur droit de contrôle sur les données les concernant:

- Information sur les traitements effectués : recueil du consentement notamment ;
- Exercice du droit de contrôle sur les données collectées : droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement ;
- L'explicitation des procédures pourra passer par des moyens humains, par exemple la mise en place d'un guichet, et d'une personne compétente ou des moyens technologiques, par exemple la mise en place d'un ensemble de pages spécifiques sur les sites des C.T.

- La centralisation : les pratiques des C.T très souvent font que des données ne sont pas partagées entre les services, sauf si ces données sont en lien avec le même métier. La numérisation offre l'opportunité pour les données à caractère médical de créer un dossier numérique unique, sécurisé et partagé par les professionnels qui suivent la personne concernée. Ce dossier médical numérique unique permettrait d'éviter la multiplication des fichiers et des procédures de déclaration auxquelles sont soumis les administrés, l'éventuelle non-concordance des données entre les déclarations, un niveau de sécurité différent dû aux multiples acteurs avec des réflexes de sécurité propres. L'opportunité de créer un dossier médical et social permettant le partage du secret entre professionnels, et la consultation par la personne elle-même nous apparait comme une préconisation essentielle. Elle permettrait un dossier unique, de référence, tenu à jour, sécurisé, et dont les accès seraient fonction des responsabilités des professionnels concernés.

f) Prioriser les actions portant sur les données sensibles.

La mise en œuvre du RGPD implique une transformation profonde du travail des élus et des agents des collectivités locales en ce qui concerne les processus de traitement des données, l'organisation de ces C.T (désignation d'un DPO et mise en œuvre de ses missions) et, au-delà, de leur culture administrative (responsabilisation face au traitement des données). Une telle mutation ne pourra pas s'accomplir du jour au lendemain. En pratique, l'adaptation au nouveau cadre sera progressive et des processus d'essais-erreurs seront inévitables. C'est pourquoi, il convient pour les collectivités locales d'aller à l'essentiel, c'est à dire d'engager leur transformation en agissant le plus tôt possible pour sécuriser les traitements de données qui font courir les risques les plus importants aux libertés des personnes concernées[7].

L'identification des traitements à sécuriser en priorité peut se fonder soit sur la nature des données traitées, soit sur l'objet du traitement.

7 Voir en particulier sur ce point les documents très précieux de la CNIL : https://www.cnil.fr/fr/organiser-les-processus-internes

- La nature des données traitées : au sein de l'ensemble des données personnelles qui font l'objet de traitements par les collectivités locales, les données sensibles sont celles dont la protection doit être assurée prioritairement : données relatives à la santé, aux infractions, aux mineurs, aux opinions politiques, syndicales, religieuses…, aux informations génétiques ou biométriques.
- L'objet du traitement : devront être prioritaires les traitements aboutissant à des décisions modifiant la situation juridique ou les droits d'une personne physique, à la création de fichiers pouvant porter atteinte à des libertés publiques (surveillance à grande échelle d'une zone accessible au public), au croisement d'ensembles de données personnelles, à l'usage de données personnelles dans des systèmes technologiques innovants…

Recommandations :

Dans ces domaines où les risques d'atteinte sont les plus importants, les collectivités locales devront engager des actions immédiates :

- Mener une analyse d'impact sur la protection des données : données à protéger, impacts potentiels, sources de risques, vulnérabilité de la chaîne du traitement ;
- Vérifier le fondement juridique sur lequel repose le traitement : obligation légale, intérêt légitime, consentement des personnes concernées ;
- S'assurer que le principe de transparence est respecté ;
- Fournir à la personne concernée les informations relatives aux données collectées et à leur traitement (art.13 et 14) ;
- Veiller à ce que les personnes concernées puissent exercer les droits qu'elles tiennent des articles 15 et suivants : accès, rectification, effacement, limitation du traitement, portabilité… ;
- Veiller à ce que les éventuels sous-traitants soient en conformité avec les obligations résultant du RGPD par l'insertion des clauses adaptées dans les contrats de sous-traitance ;
- En cas d'incident, veiller à ce que les obligations de notification soient mises en œuvre dans les délais prévus[8].
- Egalement mettre en place des processus de traitements de données sensibles très sécurisés, comme par exemple l'obligation d'avoir des mots de passe complexes.
- Il serait recommandé de créer un dossier médical numérique unique à une personne, qui soit sécurisé, dont la vocation serait d'être partagé par les professionnels concernés par la personne (personnel de la santé, pompiers, instituteurs et éducateurs, assistantes sociales, etc.). Les droits d'accès seraient différents en fonction de leurs compétences et responsabilités. Cela permettrait à la fois de ne remplir qu'un questionnaire par personne en évitant les oublis et les non mises à jour, mais également de le centraliser pour son stockage, de tracer son utilisation.

8 https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

3) Le Data Protection Officer (DPO)

Le cadre du RGPD impose la nomination d'un Data Protection Officer (DPO). Si les grandes communes ont lancé une réflexion sur le sujet, les intercommunalités interrogées et les petites communes sont quant à elles dépassées par cette nouvelle obligation de nommer un DPO et ne se sont pas encore intéressées à ce sujet. En outre, leur principale crainte est budgétaire, car aucune d'elles n'a de financement pour la création d'un nouveau poste ou pour l'application du RGPD de façon générale.

Mais regardons quel pourrait être le positionnement du DPO dans la structure et les moyens qui seront mis à sa disposition.

a) Le RGPD, une logique de protection peu adaptée aux petites collectivités locales

Le RGPD ne modifie pas substantiellement la notion de « données à caractère personnel ». En revanche, il introduit une révolution copernicienne pour ce qui est de leur protection. La culture administrative française avait conduit à un régime de protection fondé sur un dispositif de contrôle préalable par une autorité indépendante des traitements informatiques réalisés sur des données personnelles. Pour les collectivités territoriales, ce mécanisme présentait l'avantage de la sécurité, la conformité ou l'absence de conformité du traitement envisagé étant reconnue explicitement avant même qu'il ne soit mis en place. En rupture avec cette logique, le RGPD a mis un terme à cette logique de contrôle a priori pour instaurer une logique dite de « responsabilisation » dans laquelle les collectivités locales doivent s'assurer par elles-mêmes de la conformité des traitements opérés sur les données personnelles au regard des règles du droit positif. Pour ce faire, le RGPD impose la nomination d'un Délégué à la Protection des Données qui prend la succession du Correspondant Informatique et Liberté mais avec des missions et des responsabilités très élargies.

Pour les collectivités locales, cette logique de « responsabilisation » est un facteur de complexité et de coût.

Complexité tout d'abord car les attentes à l'égard des collectivités locales se multiplient et introduisent dans certains cas des formes de dissonance cognitive. Ainsi, l'ouverture des données publiques ou la transparence financière, voire la dématérialisation comptable prévues par la loi NOTRe induisent un développement considérable des traitements et des usages portant sur des données numériques à caractère personnel alors que les systèmes de traitement automatisés sont victimes d'attaques cybernétiques de plus en plus nombreuses et de plus en plus complexes et que la responsabilité des élus et des agents se trouve très largement renforcée. Coût ensuite car, dans les plus grandes des collectivités locales, ce défi est relevé grâce à des ressources humaines et des budgets d'équipement ou de fonctionnement importants. Dans les plus petites, le manque de ressources humaines et de ressources techniques ou financière risque de conduire à des vulnérabilités criantes et la mise en cause d'élus ou d'agents à qui seront reprochés alternativement la rétention d'informations qui devraient être mises à la disposition du public au titre de l'ouverture des données publiques ou l'insuffisante protection de données personnelles qui se retrouvent dans le domaine public.

b) Le DPO, une ressource inaccessible pour les petites collectivités locales

La désignation d'un Délégué à la Protection des Données (ou DPO) est obligatoire pour toutes les collectivités locales. Mais, une lecture même rapide des attributions et des conditions de désignation d'un Délégué fait apparaître que l'immense majorité des collectivités locales sera totalement incapable d'assumer par elle-même le coût d'un tel dispositif.

Dans la logique de responsabilisation retenue par le RGPD, le Délégué joue, en effet, un rôle de conseil et de contrôle extrêmement étendu. Ses principales missions sont les suivantes :

- Diffuser une culture « Informatique & Libertés » au sein de la collectivité ;
- Informer et conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents ;
- Conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- Contrôler le respect du règlement et du droit national en matière de protection des données, en particulier, mais pas seulement grâce à la réalisation d'audits ;
- Coopérer avec la CNIL et être le point de contact de celle-ci.

Pour veiller à l'effectivité du dispositif ainsi mis en place, le RGPD impose certaines conditions dans le choix du Délégué. Celui-ci doit :

- Etre désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- Etre associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés ;
- Bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Le profil d'un Délégué à la Protection des Données est donc celui d'un expert technico-juridique, capable de prendre la mesure d'une architecture de traitement automatisée des données, d'en percevoir les fragilités potentielles, de recommander les mesures à prendre dès la conception des traitements pour garantir la protection des données, de vérifier la conformité des usages aux normes et règles en vigueur, de répondre aux demandes de conseil des élus… Les ressources de ce type sont rares ; elles seront coûteuses. On peut en estimer la charge annuelle à celle d'un cadre de bon niveau. Face à l'évidente impossibilité pour les collectivités locales les plus nombreuses de se doter de « l'homme-orchestre » du traitement des données personnelles qu'est le Délégué à la Protection des Données, les petites collectivités n'ont que deux solutions : l'externalisation et la mutualisation.

c) L'externalisation, une solution qui déplace le problème

Le RGPD a créé une obligation et une forme de menace pour les collectivités locales ; il a créé une opportunité pour un certain nombre d'acteurs qui se sont « découverts » une vocation de protection des données personnelles de leurs concitoyens.

S'agissant d'une mission qui requiert une double compétence à la fois technique (expertise en sécurité des systèmes d'information et en cyber sécurité) et juridico-administrative (expertise en droit et en gouvernance des procédures de traitement), nombre de cabinets juridiques et de

prestataires informatiques se sont positionnés sur le marché et offrent leurs services aux collectivités locales. Ces cabinets mettent en avant un double avantage en termes de compétence et de coût.

Sur le second point, l'avantage procuré par l'externalisation est la possibilité de moduler, voire de variabiliser, le coût du DPO pour la collectivité locale. Il n'est pas certain que, par exemple, toutes les communes françaises aient besoin d'un DPO à plein temps tout au long de l'année. Le recours à un prestataire extérieur permet de définir un volume horaire hebdomadaire, mensuel ou annuel adapté aux besoins de la commune. La charge fixe que représenterait un cadre à plein temps peut être remplacée par une charge modulaire dont le coût peut être estimé aux alentours de 1000 euros la journée. Dès lors qu'une petite commune n'aura besoin que de l'intervention d'un DPO de l'ordre de quelques semaines par an, le coût d'une prestation externalisée, sans être insignifiant, présentera un avantage certain.

En ce qui concerne la question de la compétence, une double question se pose. En effet, l'avantage de coût résultant de l'externalisation de la prestation n'a de sens que si le service rendu répond aux exigences du RGPD et aux attentes en termes de protection effective des données personnelles.

Or, d'une part, l'offre de service en matière de protection des données ne fait l'objet d'aucune condition d'entrée. Il n'est pas exigé des offreurs qu'ils détiennent un certain diplôme ou niveau de formation comme dans les professions réglementées. Il n'est pas non plus prévu de labels ou de listes de prestataires agréés. Ce sera donc au marché de faire le tri entre les offreurs et d'éliminer les moins bons au profit des meilleurs. Il serait ici possible de suggérer un accompagnement du marché de sorte que le tri intervienne dans les meilleurs délais et avec le moins d'erreurs possibles. Des formules de classement existent aujourd'hui pour les hôtels, les lycées ou les hôpitaux. On pourrait imaginer qu'il en soit de même pour les DPO. Une labellisation pourrait être envisagée par l'ANSSI comme elle existe pour certains prestataires dits « de confiance ». Les communes pourraient également partager leur expérience, notamment en cas de difficulté significative.

D'autre part, l'externalisation ne présente un véritable intérêt pour les collectivités locales qu'à la condition qu'elles maîtrisent les conditions dans lesquelles celle-ci se produit. C'est sur ce point que la mise en place d'un DPO externalisé risque, dans de nombreux cas de déplacer le problème plus qu'elle ne le résoudra. En effet, les petites communes qui n'auront pas la compétence ni les moyens de recruter un DPO par elles-mêmes n'auront pas davantage la compétence et les ressources pour négocier et suivre le contrat : définition du besoin et de la prestation adaptée, vérification de la compétence effective du prestataire, contrôle de ses installations techniques, rédaction des engagements souscrits par les deux parties… En l'absence de toute aide extérieure (labellisation, conditions d'accès, contrats types…), les communes les plus petites mais les plus nombreuses, seront en difficulté pour assurer le degré de protection voulu par le RGPD.

d) Les mesures nécessaires pour instaurer une relation saine avec un DPO extérieur

Bien qu'il soit source de difficultés, le recours à un DPO externalisé sera probablement une solution commune pour les collectivités locales qui n'ont pas la taille requise pour se doter de ressources propres et qui n'appartiennent pas à des intercommunalités, des départements ou des régions ayant mis en place des solutions de mutualisation. Il sera encouragé par une offre de prestations pressante, la peur des sanctions et la probable médiatisation d'actions judiciaires menées par des citoyens ou des associations en vue du respect des obligations nouvelles instaurées par le RGPD.

L'externalisation de la mission de protection des données et le recours à un prestataire extérieur n'est pas en soi une solution à écarter. Elle peut parfaitement répondre aux besoins d'une collectivité qui n'effectue que des traitements de base sur les données personnelles concernant une population limitée et qui n'aurait, en tout état de cause, ni la nécessité ni les moyens de disposer d'un DPO à temps complet.

Voici deux écueils à éviter d'une telle solution :

Un prestataire qui ne dispose pas des ressources matérielles et / ou des compétences pour assurer le service promis. En l'occurrence, le volume des données que la commune confie au prestataire pour sa sauvegarde excède le volume que ce dernier est en capacité de stocker. Les dernières sauvegardes n'effacent pas les premières. Aucune alerte ne semble se déclencher pour signaler le problème. Au total, lorsque la mairie est victime d'une attaque de type « Ransomware », il semble que le prestataire découvre que les données des six derniers mois d'activité n'ont pas été sauvegardées et sont perdues irrémédiablement. On peut considérer que le prestataire ne s'est pas montré à la hauteur d'une mission qui n'était pourtant pas d'une très grande complexité.

Une commune qui ne dispose pas des compétences requises pour instaurer une relation saine avec le prestataire extérieur. Il faudrait, en effet, que la commune soit en mesure de vérifier si la prestation proposée répond au besoin exprimé et si le prestataire est en mesure de remplir effectivement la mission qui lui est confiée. Il faudrait donc qu'elle dispose non seulement des compétences techniques qui font précisément qu'elle recourt à une expertise extérieure (vérifier l'équipement du prestataire, ses ressources humaines, ses procédures…) et, en outre, de compétences juridiques pour établir un contrat adapté et équilibré. En l'espèce, le devis est formulé en des termes pour le moins généraux et les obligations du prestataire demeurent assez peu précises.

Le problème est classique et les solutions le sont tout autant.

La première consiste dans le libre jeu du marché et des mécanismes de réputation. Sur le marché émergent des DPO, les offres de service seront très diverses : avocats spécialisés, sociétés de services en informatique ou de conseil en organisation… Des acteurs majeurs, éventuellement des sociétés multinationales de conseil, seront sur les rangs et occuperont probablement le créneau des villes de moyenne / grande importance. Mais, le marché des petites communes sera plus probablement le fait d'acteurs locaux dispersés et de petites dimensions. Tous ne disposeront pas des mêmes ressources ni des mêmes compétences. La libre circulation de l'information combinée avec la liberté de choix du prestataire conduira à une sélection des offres les plus pertinentes.

A défaut de mesures d'hétéro-régulation volontaristes, c'est ce mécanisme de la sélection marchande qui assurera le tri entre les prestataires et garantira l'émergence d'une offre de qualité sur le marché de la protection des données. Si l'on considère que ce processus de sélection est trop lent et qu'il se paye de pertes ou de fuites de données personnelles insupportables, il convient alors de l'accompagner par des mesures visant à introduire des signaux externes dans le jeu de la concurrence. Ces signaux pourraient consister en des mesures multiples intervenant en amont ou en aval.

- Procédure d'agrément préalable : il s'agirait d'instaurer une évaluation a priori, sorte de procédure d'agrément délivrée aux prestataires qui entendent proposer des offres sur le

marché. L'administration centrale (ANSSI), une autorité administrative indépendante (CNIL), une organisation professionnelle ou les Régions pourraient être dotées du pouvoir d'inscrire sur des listes de prestataires agréés les personnes présentant des garanties de compétence minimale, notamment en termes de formation juridique et technique.

- Obligation d'assurance : les prestataires agréés (ou non) pourraient se voir imposer une obligation d'assurance professionnelle visant à couvrir leurs clients contre les fautes commises dans l'exercice de la mission. Le mécanisme de sélection serait ainsi reporté sur ces compagnies d'assurance toujours soucieuses d'ajuster le montant des primes au risque induit par l'assuré, ce qui conduirait à faire peser sur les moins bons d'entre eux un coût supplémentaire susceptible de les dissuader de continuer.
- Evaluation extérieure : l'époque est à l'évaluation de tous par tous. Le secteur de l'hôtellerie est sous la férule de « Tripadvisor », les universités subissent le « classement de Shangaï » et les hôpitaux ou les lycées, le hit-parade du journal « Le Point ». Les technologies disponibles favorisent la mise en ligne des opinions et des commentaires et l'on pourrait imaginer qu'une association de citoyens ou d'élus locaux développe un « comparateur » des prestataires auquel pourraient se référer les communes souhaitant externaliser la mission du DPO qu'elles ne peuvent pas recruter. Cette pratique se heurterait sans doute à des limites juridiques, notamment dans la manière de concevoir l'outil, mais elle ne paraît pas impossible à mettre en place.
- Procédures judiciaires : last but not least, le RGPD prévoit des sanctions en cas de non-conformité des politiques et des mesures de protection des données personnelles. Ici aussi, l'activisme judiciaire de certaines associations peut laisser penser que des poursuites seront engagées et que certaines auront une portée médiatique significative produisant un effet de « Name and Shame » à la fois pour la commune et pour le prestataire dont l'image sera ainsi dégradée auprès des prospects qu'il pourra solliciter.

Ces différentes mesures ne sont pas exclusives les unes des autres. Leur adoption suppose une volonté politique puisqu'il s'agit de déroger au principe de la libre entreprise et du jeu « naturel » du marché. Mais, les dommages résultant de la carence d'un prestataire seront sans doute assez importants pour que l'autorégulation de ce marché ne soit la seule procédure de sélection admissible.

e) La mutualisation, une solution qui pose la question de l'équilibre des pouvoirs entre les collectivités locales

La Loi NOTRe a renforcé le rôle des intercommunalités, par exemple de gestion de l'eau, d'assainissement ou de gestion des déchets. La logique de rationalisation des moyens en vue de rendre des services plus efficaces aux habitants de collectivités qui ont des besoins identiques s'applique parfaitement à la protection des données personnelles. Il serait dès lors concevable d'externaliser la fonction de DPO non pas vers un acteur singulier proposant une offre sur le marché mais vers les structures de mutualisation informatiques qui existent déjà et portent généralement les développements des infrastructures et des processus de dématérialisation dans leurs territoires respectifs.

Les avantages sont ceux de l'externalisation dont la mutualisation n'est que l'une des formes particulières : partage du coût, modulation et variabilisation de la prestation, compétence d'un

organisme spécialisé… Elle peut aussi en présenter les inconvénients : inégalité des prestations, efficacité variable en matière de contrôle des coûts… La mutualisation au sein d'un service intercommunal, départemental ou régional présente toutefois la garantie d'un service dont les bénéficiaires exercent un contrôle politique sur la structure de pilotage et de gestion du prestataire.

Reste la question du bon niveau de mutualisation. Plusieurs solutions sont possibles qui impliquent des équilibres différents en termes de pouvoir.

f) Le profil du DPO

Les ressources humaines doivent définir le profil du Data Protection Officer. Ce dernier doit posséder des notions juridiques certaines ainsi qu'une expertise technique qui peut impliquer une formation. Un profil d'archiviste est tout à fait envisageable pour ce type de poste, sachant que la valorisation du patrimoine documentaire passe par l'acquisition de compétences numériques et la maîtrise d'outils numériques.

g) Accompagnement du DPO : structure régionale de soutien

L'arrivée d'un DPO au sein de l'organisation n'est pas aussi simple qu'il n'y parait. En effet, ses missions le mettent dans une position de contrôle de conformité des pratiques au sein de la collectivité qui l'emploie et donc de l'ensemble du personnel. La collectivité ne fait finalement que l'employer car de fait, c'est bien à l'instance référente (type Cnil) que celui-ci devra faire un reporting et/ou signaler les manquements.

Du coup, la relation hiérarchique devient complexe. Le DPO pourra contrôler son supérieur dans la structure et signaler les anomalies. Ces relations créeront une ambiance de méfiance, voire de blocage au sein de la structure, puisqu'il devra aussi veiller aux bonnes pratiques de ses collègues et en référer à qui de droit.

Les quelques collectivités moyennes avec qui nous avons abordé les différentes possibilités d'organisation et de gouvernance du DPO, s'accordent sur l'idée d'externaliser le service. Et ce, pour 2 raisons : pour éviter des tensions internes des 2 bords (blocage des agents contrôlés et rétention d'informations, rendant la mission du DPO difficile), et pour réduire la charge financière d'un DPO en interne. Les solutions seraient la collaboration avec un cabinet d'avocat, ou bien de partager un DPO basé dans une structure externe.

Dans le cas où la C.T fait le choix d'un DPO en interne, il est recommandé de lui réserver un statut à part qui le protège des liens hiérarchiques avec les collègues de la structure. Un référent hiérarchique externe semble une piste à explorer. Ce peut être un organisme régional, tel que développé plus haut dans le rapport. Son emploi du temps pourrait dans ce cas être partagé entre plusieurs structures.

La structure régionale deviendrait, de ce fait, le référent vis-à-vis de la structure nationale lors de signalement de non-conformité ou de manquements, de préconisations ou de demandes spécifiques.

Le DPO pourrait, partiellement, être détaché dans les C.T. Ce principe d'organisation et de lien hiérarchique vaut pour le DPO mis à disposition par l'intercommunalité ou le Centre de Gestion d'un département.

Il semble nécessaire de définir également quelques spécificités liées à ce nouveau métier avant de lancer des campagnes de recrutement des DPO en France (besoin estimé de 30 000 postes, toutes structures confondues – entreprises, administrations, organisations, CT, etc :

- Quel cadre salarial ?
- Quel cadre juridique d'intervention ?
- Quelles formations diplômantes ?
- Quel contrat de travail ?

Tout ceci mérite d'être encore éclairé en amont au risque si ce n'est pas anticipé de provoquer une belle confusion dans les structures contrôlées ! N'oublions pas que les collectivités territoriales sont très indépendantes dans leurs décisions et n'apprécient pas les intrusions dans leur gestion. La venue d'un contrôleur en leur sein sera forcément mal perçue, au début au moins.

h) L'identité numérique comme nouvel acteur de la gestion des données personnelles ?

Les Estoniens disposent depuis 2002 d'une carte d'identité électronique qui est un moyen sécurisé pour valider en ligne des documents administratifs, des accords commerciaux, des virements bancaires et bien d'autres documents.

Une telle carte pourrait contenir les données personnelles individuelles telles que définies au début de ce document, c'est-à-dire les coordonnées physiques de la personne (comment la joindre physiquement), les coordonnées numériques (comment la joindre numériquement), ainsi que les données de l'état civil (date et lieu de naissance, situation maritale) et données biométriques (empreintes digitales, photographie, iris de l'œil, etc.). Elle permettrait à l'usager citoyen de bénéficier plus aisément de certains accès à des services fournis par des C.T ou par l'État.

Recommandations :

- Les auteurs recommandent de se poser la question de l'impact de la création d'une identité numérique sur la gestion des données personnelles par les C.T en France. Une étude sur le sujet serait nécessaire, si elle n'a pas encore été lancée.

i) La piste de l'anonymisation des données personnelles

Une autre solution envisagée par la loi est l'anonymisation des données personnelles. Ainsi, il est possible de rendre public les documents faisant intervenir des données à caractère personnel ou sensible après avoir occulté ces dernières. Cependant, cette anonymisation a un coût, à la fois matériel, humain et financier. Le projet de loi sur la République numérique le prend en compte, et

fixe des limites à l'obligation de diffusion de certaines données trop difficiles à occulter pour les collectivités territoriales.

VI. Conclusions

Les collectivités territoriales ont le sentiment d'être livrées à elle-même face à cette nouvelle obligation de mise en conformité au Règlement européen sur la protection des données. Elles sont fortement en attente d'un accompagnement et soutien.

Il est probable que pour certaines collectivités territoriales, étant donné les contraintes comme les moyens financiers insuffisants, le manque de ressources ou une expertise interne inexistante, l'externalisation de la fonction de DPO sera une solution. Cette externalisation des DPO impliquera une dépendance possible avec des prestataires extérieurs et une externalisation de l'expertise juridique.

Pour d'autres, elles nommeront au poste de DPO une personne exerçant déjà une fonction au sein de la collectivité. La case sera ainsi « cochée », mais impliquera une surcharge de travail en plus des autres fonctions que la personne exerce. A noter qu'elle n'aura pas forcément d'emblée une expertise efficace et applicable, ni le temps pour mettre en œuvre une vraie politique de protection. Ce manque de compétences et de moyens pour mener son action pourrait fragiliser la position des C.T dans l'hypothèse d'un recours exercé par un administré.

Les C.T étant constituées d'hommes et de femmes désireux de servir au mieux leur territoire, elles sont néanmoins sujettes au « facteur générationnel » qui fait que beaucoup d'élus ou d'agents ont peur de cette révolution numérique. Il convient donc de les accompagner et non pas de les forcer à subir cette transformation.

Enfin il semble aux auteurs de ce rapport que, au-delà des recommandations qui forment la cinquième partie de ce rapport, cette étude doit permettre d'aboutir à une stratégie nationale d'accompagnement des collectivités locales pour qu'elles puissent saisir l'opportunité de la numérisation et non pas la subir. En final, il est souhaitable que cet accompagnement soit déclinable rapidement et localement, notamment au profit des petites communes qui sont les plus fragiles face l'enjeu de la protection des données personnelles.

VII. Annexes

ANNEXE 1 : Tableau synthétique des compétences des collectivités territoriales françaises et de leurs groupements

Reforme_territoriale
_tableau des compétences

ANNEXE 2 : lettre d'engagement pour la protection de l'information de la ville de Vannes

Lettre d'engagement
à la protection de l'information